虚拟专用网的保证服务质量的系统及其方法

技术领域

本发明涉及虚拟专用网络的服务质量实现方案，特别涉及使用多协议标签交换的虚拟专用网的服务质量实现方案。

背景技术

虚拟专用网（Virtual Private Networking，简称“VPN”）是指在公共网络中建立专用网络，数据通过安全的“加密通道”在公共网络中传播。企业只需要租用本地的数据专线，连接上本地的 Internet（因特网），各地的机构就可以互相传递信息；同时，企业还可以利用 Internet 的拨号接入设备，让自己的用户拨号到 Internet 上，就可以连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等优点。

多协议标签交换（Multi-protocol Label Switch，简称“MPLS”）是由思科公司（CISCO）的标记交换（Tag Switching）演变而来的国际互联网工程任务组（Internet Engineering Task Force，简称“IETF”）的标准协议。MPLS 是基于标签的互联网协议（internet Protocol，简称“IP”）路由选择方法，它属于第三层交换技术，引入了基于标签的机制，把选路和转发分开，由标签来规定一个分组通过网络的路由，数据传输通过标签交换路径（Label Switch Path，简称“LSP”）完成，它将原本在 IP 网络的第三层的包交换转换成第二层的包交换。在标签中，包含一个 3 比特的 EXP 字段用来实现 QoS。

图 1 示出了 MPLS 网络结构。MPLS 网络 101 由核心部分的标签交换路由器 104（Label Switch Router，简称“LSR”）、边缘部分的标签边缘路由器 103（Label Edge Router，简称“LER”）组成。其中 LER 103 用于分析 IP 包头，执行第三层网络功能，决定相应的传送级别和标签交换路径（Label Switch Path，简称“LSP”），它与外部

网络 102 相连接，从外部网络 102 接收外部分组交换数据包(IP 包) 105；LSR 104 用于建立 LSP，执行标签交换机制和服务质量保证（Quality of Service，简称“QoS”），转发 MPLS 网络 101 内部的分组数据包 106，它由控制单元和交换单元组成，它处在网络内部，与 LER 103 和其他 LSR 104 相连。

MPLS 的标签交换的工作流程如下：最初由标签分发协议（Label Distribution Protocol，简称“LDP”）和传统路由协议，比如开发最短路优先协议（Open Shortest Path First，简称“OSPF”）等，在 LSR 中建立路由表和标签映射表；在网络运行中，首先在 MPLS 核心网入口处的 LER 接收外部网络的 IP 包，完成第三层网络功能，并给 IP 包加上标签成为分组数据包；接着该分组数据包在 LSP 中传输。此时 LSR 不再对分组数据包进行第三层处理，只是根据其标签通过交换单元进行转发，最终达到网络另一端即出口处的 LER；最后在 MPLS 出口处的 LER 将该分组数据包的标签去掉成 IP 包后按照相应外部网络协议继续进行转发。

由于 MPLS 技术隔绝了标签分发机制与数据流的关系，因此，它的实现并不依赖于特定的数据链路层协议，进而可支持多种的物理层和数据链路层技术。目前实现了在帧中继（Frame Relay，简称“FR”）、异步传输模式（Asynchronous Transfer Mode，简称“ATM”）和点到点协议（Point-to-Point Protocol，简称“PPP”）链路以及国际电气电子工程师协会（Institute of Electrical and Electronics Engineers，简称“IEEE”）802.3 协议的局域网上使用 MPLS 的业务。采用 MPLS 网络进行 IP 业务转发，可以简化层与层之间的路由转发过程，加快 MPLS 交换速度，提高网络效率，同时能满足不同等级业务的传送，所以说 MPLS 既有交换机的高速度与流量控制能力，又具备了路由器灵活的功能和服务质量保证机制。

MPLS 已经被广泛应用于 VPN 的实现，借助 MPLS 实现的 VPN 被称为 MPLS VPN。根据网络设备转发依据的用户信息，MPLS VPN 可以划

分为 L3（层 3，即网络层） VPN，L2（层 2，即数据链路层） VPN，L1（层 1，即物理层）VPN 三种类型。目前在互联网工程任务组（INTERNET ENGINEERING TASK FORCE，简称“IETF”）标准组织中，有 L3 VPN 工作组和 L2 VPN 工作组，分别研究 MPLS L3 VPN 和 MPLS L2 VPN。MPLS L3 VPN 的典型代表是基于 RFC 2547bis 的边界网关协议（Border Gateway Protocol，简称“BGP”）/MPLS VPN 和基于虚拟路由器（Virtual Router，简称“VR”）的 IP VPN。MPLS L2 VPN 的典型代表是 MARTINI，KOMPELLA，以及多种虚拟专用局域网子网段（Virtual Private LAN Segment，简称“VPLS”）实现方案。此外，国际电信联盟-电信标准部（International Telecommunication Union Telecommunication Standardization Sector，简称“ITU-T”）的 SG13/Q11 对 L1 VPN 的研究比较多，目前有 Y.11vpnarch，Y.11vpnsdr 等草案建议。他们的参考模型的结构都类似，对于 VPN QoS 问题的处理都类似，要么没有考虑，要么是利用网络自身的 DiffServ（差异服务模式）能力，因此都不能解决 VPN 的 QoS 问题，而且不能解决该问题的原因也相同，在这方面可以将他们归为相同的技术。

下面以 RFC2547bis 作为这一类技术的代表对现有技术进行说明，由于他们和 ITU-T，IETF 的 L2 VPN 和 L3 VPN 的参考模型具有相同的结构，在解决 QoS 问题上的困难是相同的。

RFC2547bis 所定义的 MPLS L3VPN 模型如图 2 所示，该模型包括三个组成部分：用户网边缘路由器（Custom Edge Router，简称“CE”）、骨干网边缘路由器（Provider Edge Router，简称“PE”）和路由器（P）。

CE 设备是用户驻地网络的一个组成部分，有接口直接与运营商的网络相连，一般是路由器。CE “感知” 不到 VPN 的存在，也不需要维护 VPN 的整个路由信息。

PE 路由器即运营商边缘路由器，是运营商网络（也称之为骨干网）的边缘设备，与用户的 CE 直接相连。MPLS 网络中，对 VPN 的所有处

理都在 PE 路由器上完成。

路由器(P)是运营商网络中的骨干路由器，它不和 CE 直接相连。路由器（P）需要有 MPLS 基本信令能力和转发能力。

CE 和 PE 的划分主要是从运营商与用户的管理范围来划分的，CE 和 PE 是两者管理范围的边界。

CE 与 PE 之间使用外部边界网关协议（Exterior Border Gateway Protocol，简称“EBGP”）或是内部网关协议（Interior Gateway Protocol，简称“IGP”）路由协议交换路由信息，也可以使用静态路由。CE 不必支持 MPLS，不需要感知 VPN 的整网路由，VPN 的整网路由外包给运营商来完成。运营商 PE 设备之间通过多协议内部网关协议（Multi-protocol Internal Border Gateway Protocol，简称“MP-IBGP”）交换 VPN 的整网路由信息。

以下介绍 RFC2547bis 标准规定的 MPLS L3VPN 的相关属性:

VRF:

VPN 是由多个站点(Site)组成的。在 PE 上，每个站点对应一个虚拟专用网路由/转发实例（VPN Routing/Forwarding instance，简称“VRF”），它主要包括：IP 路由表、标签转发表、使用标签转发表的一系列接口以及管理信息（包括路由识别号、路由过滤策略、成员接口列表等）。

(修改理由：上述说明用户站点是 VPN 的一个组成部分，用上述的话来描述会导致描述不清楚的，因此删除)一个站点可以同时属于多个 VPN。在实现中，每一个站点至少关联一个单独的 VRF。VPN 中站点的 VRF 实际上综合了该站点的 VPN 成员关系和路由规则。报文转发信息存储在每个 VRF 的 IP 路由表和标签转发表中。系统为每个 VRF 维护一套独立的路由表和标签转发表，从而防止了数据泄漏出 VPN 之外，同时防止了 VPN 之外的数据进入。

VPN-IPv4 地址族:

PE 路由器之间使用 BGP 来发布 VPN 路由，并使用了新的地址族——VPN-IPv4 地址。

一个 VPN-IPv4 地址有 12 个字节，开始是 8 字节的路由识别号（Route Distinguisher，简称“RD”），后面是 4 字节的 IPv4 地址。PE 使用 RD 对来自不同 VPN 的路由信息进行标识。运营商可以独立地分配 RD，但是需要把他们专用的自治系统（Autonomous System，简称“AS”）号作为 RD 的一部分来保证每个 RD 的全局唯一性。RD 为零的 VPN-IPv4 地址同全局唯一的 IPv4 地址是同义的。通过这样的处理以后，即使 VPN-IPv4 地址中包含的 4 字节 IPv4 地址重叠，VPN-IPv4 地址仍可以保持全局唯一。

PE 从 CE 接收的路由是 IPv4 路由，需要引入 VRF 路由表中，此时需要附加一个 RD。在通常的实现中，为来自于同一个用户站点的所有路由设置相同的 RD。

Route Target（路由目标）属性：

Route Target 属性标识了可以使用某路由的站点的集合，即该路由可以被哪些站点所接收，PE 路由器可以接收哪些站点传送来的路由。与 Route Target 中指明的站点相连的 PE 路由器，都会接收到具有这种属性的路由。PE 路由器接收到包含此属性的路由后，将其加入到相应的路由表中。

PE 路由器存在两个 Route Target 属性的集合：一个集合用于附加到从某个站点接收的路由上，称为 Export Route Targets（输出路由目标）；另一个集合用于决定哪些路由可以引入此站点的路由表中，称为 Import Route Targets（输入路由目标）。

通过匹配路由所携带的 Route Target 属性，可以获得 VPN 的成员关系。匹配 Route Target 属性可以用来过滤 PE 路由器接收的路由信息。

VPN 报文的转发过程：

在 RFC2547bis 标准中，VPN 报文转发使用两层标签方式。第一层（外层）标签在骨干网内部进行交换，代表了从 PE 到对端 PE 的一条 LSP，VPN 报文利用这层标签，就可以沿着 LSP 到达对端 PE。从对端 PE 到达 CE 时使用第二层（内层）标签，内层标签指示了报文到达哪个站点，或者更具体一些，到达哪一个 CE。这样，根据内层标签，就可以找到转发报文的接口。特殊情况下，属于同一个 VPN 的两个站点连接到同一个 PE，则如何到达对方 PE 的问题不存在，只需要解决如何到达对端 CE。

通过 BGP 发布 VPN 路由信息：

在 RFC2547bis 标准中，CE 与 PE 之间通过 IGP 或 EBGP 来传播路由信息，PE 得到该 VPN 的路由表，存储在单独的 VRF 中。各个 PE 之间通过 IGP 来保证通常 IP 的连通性，通过 IBGP 来传播 VPN 组成信息和路由，并完成各自 VRF 的更新。再通过与直接相连 CE 之间的路由交换来更新 CE 的路由表，由此完成各个 CE 之间的路由交换。

BGP 通信在两个层次上进行：自治系统内部（IBGP）以及自治系统之间（EBGP）。PE-PE 会话是 IBGP 会话，而 PE-CE 会话是 EBGP 会话。

BGP 在 PE 路由器之间的 VPN 组成信息和路由传播，通过多协议扩展边界网关协议（Multiprotocol extensions BGP，简称“MBGP”）来实现。关于 MBGP 的详细内容可以参考 IETF 的文档 RFC2283《Multiprotocol Extensions for BGP-4》（中文名称可译为《边界网关协议－4 的多协议扩展》）。MBGP 向下兼容，既可以支持传统的 IPv4 地址族，又可以支持其他地址族（比如 VPN-IPv4 地址族）。通过MBGP 携带的 route target(路由目标)确保了特定 VPN 的路由只能被这个 VPN 的其他成员知道，使 BGP/MPLS VPN 成员间的通信成为可能。

当通过 VPN 传输数据时，用户经常指定其服务质量(QoS)。比如：指定传输数据的优先级。该传输数据的优先级越高，VPN 在保证传输

可靠性的基础上越先传输。在实际应用中，上述方案目前并未有成熟的 MPLS VPN QoS 方案，由此造成不能满足用户需求的后果。

造成这种情况的主要原因在于，由同一组 PE 接入的不同 NBVPN 之间通过复用 MPLS 标签栈中的外层标签来同享资源。虽然理论上可以通过部署 DiffServ-aware（通过 IP 的差异化服务编码点（DSCP）字段来进行不同优先级的转发）或类似的方案来保证外层隧道的资源，但在这些参考模型中，每个 VPN 中没有一个设备了解骨干网络中的资源状况，由于在每个节点几个 VPN 之间存在资源竞争，而且都不知道骨干网络中的资源状况，因此为每个 VPN 保证资源比较困难，这种共享竞争的机制给保证 VPN 的服务质量保证带来了更多复杂性。

IETF 的提供者指配的虚拟专用网（Provider Provisioned Virtual Private Networks，简称“PPVPN”）工作组在 2003 年 7 月维也纳会议后分为两个工作组：L2 VPN 和 L3 VPN，在它们最新的 charter 中，都没有包括 QoS 解决方案，它们现在的 VPN 参考模型中，QoS 问题仍然存在。在 IETF 的《draft-martini-l2circuit-trans-mpls-10.txt》和《draft-martini-l2circuit-encap-mpls-04.txt》（这两篇文稿是 L2VPN 的基础）中，对于 QoS 问题，都表示“QoS related issues are not discussed in this draft”（QoS 相关问题没有在这个草案中讨论），在《draft-ietf-l3vpn-rfc2547bis-01.txt》（该文稿是 BGP/MPLS VPN 的基础）中，对于 VPN 的 QoS 问题，只是简单的说“existing L3 QoS capabilities can be applied to labeled packets through the use of the “experimental” bits in the shim header”（现存的 L3 QoS 能力可以通过使用标签包头部的实验比特来解决），但问题是 L3 QoS 本身也是一个复杂的未解决的问题。因此，L2VPN/L3VPN 中的 QoS 问题都还没有解决。

在 2003 年 7 月份 ITU-T SG13 会议上，通过了研究通用 VPN（GVPN）的提议，草案建议 Y.nbvpn-decomp 作为通用基于网络的虚拟专用网

（Network Based Virtual Private Network，简称“NBVPN”）功能分解的初始文本，是通用虚拟专用网（Generalized Virtual Private Network，简称“GVPN”）构建块分类的基础。在 Y.nbvpn-decomp 中，对一些功能实体进行了分类，其目的是简化 VPN 问题，以便定义网络运营商提供所希望的 VPN 网络需要的技术和机制，但 Y.nbvpn-decomp 中的参考模型和相应的 QoS 问题与 IETF 提出的 VPN 参考模型和 QoS 问题都相同，因此，QoS 问题也没有很好地解决，这样，整个 VPN 模型就不会足够通用，以满足希望提供有 QoS 保证的 VPN 业务的运营商的需求，而且 VPN 用户虽然被允许接入，但不能保证向他们在使用异步传输模式（Asynchronous Transfer Mode，简称“ATM”）/帧中继（Frame Relay，简称“FR”）/数字数据网络（Digital Data Network，简称“DDN”）时得到他们需要的资源。

发明内容

有鉴于此，本发明的主要目的在于提供一种虚拟专用网中保证服务质量的系统及其方法，使得 MPLS VPN QoS 问题可以有一种实用的解决方案。

为实现上述目的，本发明提供了一种基于网络的虚拟专用网中保证服务质量的系统，包含：

逻辑承载网，使用多协议标签交换技术通过在基础 nIP 网络中配置预留带宽的标签交换路径连接各种路由器而形成，专用于传输有服务质量需求的业务；

承载控制网，用于对所述逻辑承载网进行维护并对所述业务进行路由。

其中，所述承载控制网包含集中式资源控制器，用于管理所述逻辑承载网的网络资源，维护所述逻辑承载网的网络拓扑，进行资源计算和路由选择，为所述路由器发送路由指示，在所述逻辑承载网内分配资源并进行接入控制，为每一个所述虚拟专用网维护成员关系信息

和连接关系信息，实现成员关系的自动发现和单边配置。

所述集中式资源控制器在所述逻辑承载网的每一个域中部署一个，各个所述集中式资源控制器相互连接，交流所述逻辑承载网的拓扑、资源信息以及所述虚拟专用网的路由信息。

所述逻辑承载网和所述承载控制网通过带外的方式发布所述虚拟专用网的路由、维护所述虚拟专用网的成员关系、维护所述虚拟专用网各站点之间的访问关系。

所述各种路由器包含骨干网边缘路由器、中间转接路由器与核心路由器，

所述骨干网边缘路由器用于识别有服务质量需求的虚拟专用网，对从该虚拟专用网进入的有服务质量需求的业务用所述集中式资源控制器指示的标签栈进行封装，根据该业务的优先级设置所述标签栈中所有标签的服务质量字段，将封装好的业务数据包通过所述逻辑承载网传输；

所述中间转接路由器用于实现标签交换路径的静态或动态配置、区别服务模式的多协议标签交换和按类型处理流的功能；

所述核心路由器用于实现区别服务模式的多协议标签交换和按类型处理流的功能。

所述集中式资源控制器包含接口管理模块、协议处理模块、成员关系维护模块、拓扑和资源管理模块、路由管理模块和自动发现信令模块，

所述接口管理模块用于实现并管理和外部设备进行通信的接口；

所述协议处理模块用于对所述集中式资源控制器与各种外部设备通信的协议进行处理，并根据协议要求将通信数据转发给所述成员关系维护模块、拓扑和资源管理模块、路由管理模块和自动发现信令模块，所述协议处理模块通过所述接口管理模块收发通信数据；

所述成员关系维护模块用于维护所述虚拟专用网的成员关系信息和所述虚拟专用网站点间访问关系信息;

所述拓扑和资源管理模块用于管理所述逻辑承载网的拓扑关系和资源;

所述路由管理模块用于管理所述虚拟专用网的路由关系;

所述自动发现信令模块用于变更的自动发现,并通知所述成员关系维护模块、所述拓扑和资源管理模块修正相应的信息。

本发明还提供了一种基于网络的虚拟专用网中保证服务质量的方法,包含以下步骤:

A 在基础 IP 网络中,使用多协议标签交换技术通过配置预留带宽的标签交换路径构造逻辑承载网,该逻辑承载网专用于有服务质量需求的业务;

B 部署用于集中管理所述逻辑承载网资源的集中式资源控制器;

C 需要传输有服务质量需求的业务时,将该业务的优先级标记到封装该业务数据流的多协议标签交换数据包的路由标签的服务质量字段中,按照所述集中式资源控制器分配的路由,通过所述逻辑承载网传输。

其中,所述集中式资源控制器在所述逻辑承载网的每一个域中部署一个。

所述路由可以是由标签栈确定的串行标签交换路径。

所述步骤 C 中,对所述业务路由标签栈中全部标签的服务质量字段设置相同的数值。

所述方法还包含以下步骤:

使用多协议标签交换流量工程技术动态调整所述逻辑承载网的拓扑和资源。

在所述步骤 C 中，所述业务的优先级可以由所述业务的类型确定。

当所述虚拟专用网同时包含有服务质量需求的站点和没有服务质量需求的站点时，包含以下步骤:

判断业务的收、发站点是否都有服务质量需求，如果是则使用逻辑承载网内的资源传输该业务，否则使用所述基础 IP 网络的其他资源传输该业务。

所述对业务的收、发站点是否都有服务质量需求的判断包含以下子步骤:

E1 比较所述收、发站点的路由目标，判断所述收、发站点是否为普通访问关系，如果是则进入步骤 E2;

E2 比较所述收、发站点的有服务质量需求的路由目标，判断所述收、发站点是否为有服务质量需求的访问关系，如果是则判定所述收、发站点之间的业务具有服务质量需求，否则判定所述收、发站点之间的业务没有服务质量需求。

所述集中式资源控制器为每一对有服务质量需求的站点分配的路由是唯一。

通过比较可以发现，本发明的技术方案与现有技术的区别在于，通过在基础 IP 网络中通过MPLS 技术预配置一部分资源给 QoS-VPN 专用（称为 VPN 逻辑承载网），并在当前 VPN 参考模型中增加集中式资源控制器，用于维护 VPN-LBN 的网络拓扑和资源，以及每个 QoS-VPN 的成员关系信息和访问关系信息，并根据逻辑承载网的资源状态进行允许控制和路由计算，保证接入的业务都能得到它们希望的服务质量。

这种技术方案上的区别，带来了较为明显的有益效果，即解决了 MPLS VPN 的 QoS 问题，对于运营商开展具有 QoS 保证的 VPN 起到了推动作用；解决了 VPN 大网络运营、跨域运营中的复杂性和可规划、

可管理、可运营的特性；统一了 MPLS L3/L2/L1 VPN 的提供 QoS 的解决方案。

附图说明

图 1 是 MPLS 网络结构示意图；

图 2 是 RFC2547bis 所定义的 MPLS L3VPN 模型；

图 3A 是本发明提供的一种虚拟专用网中保证服务质量的方法的流程图；

图 3B 是根据本发明的一个实施例的实现 QoS－VPN 的方法流程图；

图 4 是根据本发明的一个实施例的 QoS-VPN 构架的参考模型；

图 5 是根据本发明的一个实施例的使用 MPLS 技术的 VPN-LBN；

图 6 是根据本发明的一个实施例的 VPN－CRC 内部结构及对外连接关系示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

请参阅图 3A，其为本发明提供的一种虚拟专用网中保证服务质量的方法的流程图。它包含以下步骤：首先，在基础 IP 网络中，使用多协议标签交换技术通过配置预留带宽的标签交换路径构造逻辑承载网，该逻辑承载网专用于传输有服务质量需求的业务(步骤 S10)；然后，部署用于集中管理所述逻辑承载网资源的集中式资源控制器(步骤 S20)；最后，当需要传输有服务质量需求的业务时，将该业务的优先级标记到封装该业务数据流的多协议标签交换数据包的路由标签栈的服务质量字段中，按照所述集中式资源控制器分配的路由，通过所述逻辑承载网路由到需发送的对端(步骤 S30)。

本发明通过在基础IP网络中通过MPLS技术预配置一部分资源给QoS-VPN专用，然后通过配置的集中资源控制器来维护其VPN-LBN的网络拓扑和资源，以各种成员关系信息和访问关系信息；由此保证接入的业务能得到其所要求的服务质量。

现举一个实施例来说明本方法的具体实现过程。

图3B示出了实现上述方法的流程图，在步骤100，进行容量规划：将需要QoS保证的基于网络的虚拟专用网（Network Based Virtual Private Network，简称“NBVPN”）业务划分为一个特殊业务类型，本发明称之为QoS-VPN业务，这种NBVPN称为QoS-VPN，网络运营商在接入这种业务时应该能够识别这种业务，最简单的方法（当然不限于此）是在接入QoS-VPN的站点的PE上识别出这些站点连接的接口或子接口，认为从这些接口或子接口进入的业务都是QoS-VPN业务，网络运营商需要根据当前和预期的QoS-VPN业务来规划QoS-VPN业务的容量，包括拓扑，路由，带宽等。

此后进入步骤110，配置VPN－逻辑承载网（Logical Bearer NetWork，简称“LBN”）。根据容量规划的结果，使用MPLS技术在基础IP网络中预配置一个LBN给QoS-VPN单独使用，对于QoS-VPN业务流，其路由选择，资源分配，允许控制和标签转发仅在VPN-LBN中处理，对于没有QoS需求的VPN业务流，在基础网络中没有预配置的部分资源中根据现存的VPN机制进行路由和转发。

此后进入步骤120，部署VPN－集中式资源控制器（Centralized Resource Controler，简称“CRC”）。在VPN-LBN中的每个域中部署一个VPN－CRC，一般是和VPN的数据平面设备分离，VPN-CRC负责VPN站点之间的资源计算，接入控制，资源分配，路由选择，将表示路由的MPLS标签栈下发给入口PE，并为每个QoS-VPN维护成员关系信息，访问关系信息，并处理必要的信令。之所以在每一个域部署一

个 CRC 是因为如果只部署一个全局 CRC，则当网络巨大时需要协调的信息太多。域是运营商自己划分的逻辑区域，例如一个省或一个市，可以根据 CRC 的实际处理能力来决定域的范围大小。

上述实施例中，QoS-VPN 网络的拓扑和带宽是静态分配的，在本发明的另一个较佳实施例中，使用 MPLS 流量工程（Traffic Engineering，简称“TE”）技术来动态调整 VPN-LBN 拓扑和带宽，以进行 LSP 的保护或容量变更。

此后进入步骤 130，VPN-CRC 计算并下发站点之间访问路径。因为 VPN-LBN 中所有的可用资源信息以及 QoS-VPN 中的成员关系信息和访问关系信息都记录在 VPN-CRC 中，因此 VPN-CRC 可以根据这些信息为每一对有 QoS 需求的站点计算访问路径，并且把路径下发到各个 PE 中，由 PE 来具体执行。因为有这种处理方式，因此每一对有 QoS 需求的站点之间的路径都是唯一确定的。

此后进入步骤 140，标记业务优先级并通过 VPN－LBN 传输。在每个 QoS-VPN 中，虽然两个站点之间的所有业务的路由完全相同，但这些业务流仍可以分为不同类型，如语音，视频，数据，这些业务类型可以在入口 PE 识别并标记不同的优先级，在入口 PE 对这些不同优先级的数据流进行 MPLS 封装时，将优先级映射到 VPN-CRC 下发给入口 PE 的表示路由信息的标签栈中的所有标签的 EXP（因为标签栈的标签在沿着这些路由转发时要进行弹出操作，所有标签的 EXP 设置相同将可以保留业务流的优先级信息），这样在 VPN-CRC 确定了两个站点之间业务的路由和带宽后，其中不同的业务等级可以通过 MPLS-DiffServ（区别服务模式）进行转发，保证各自的时延/抖动/包丢失等要求，从而保证 VPN 的 QoS.

需要说明的是，对于混合 QoS-VPN，可以将其分成两部分，一部分由具有 QoS 要求的站点组成，上述机制可以应用于这部分，另一部

分由没有 QoS 要求的站点组成，遵循已有的 VPN 机制。即：在接收到业务时，需判断业务的收、发站点是否都有服务质量需求，如果是则使用逻辑承载网内的资源传输该业务，否则使用所述基础 IP 网络的其他资源传输该业务。并且，在对业务的收、发站点进行是否都有服务质量需求的判断前还包括以下子步骤：比较所述收、发站点的路由目标，判断所述收、发站点是否为普通访问关系，如果是则进入后续步骤，否则结束。

其中，判断业务的收、发站点是否都有服务质量需求是通过以下方式来判断的：通过比较所述收、发站点的路由目标，判断所述收、发站点是否为有服务质量需求的访问关系，若是，则业务的收、发站点都有服务质量需求，否则，业务的收、发站点未有服务质量需求。

下面结合图 4 说明 QoS－VPN 的总体框架。

在本发明的一个较佳实施例中，QoS-VPN 框架分为两个层次：逻辑承载网（logical bearer layer，也可以成为逻辑承载层），承载控制网（bearer control layer）。逻辑承载层是使用 MPLS 技术根据预先的容量规划通过配置预留带宽的 LSP 连接 PE，CR，ITR 形成的。

承载控制网由若干个 VPN-CRC 组成，每个域配置有一个 VPN-CRC（不包括 VPN-CRC 的备份），VPN-CRC 管理 VPN-LBN 的网络资源（包括带宽，处理器，缓冲区），维护 VPN-LBN 的网络拓扑，进行资源计算，路由选择，给 PE 发送路由指示，在 VPN-LBN 内分配资源，接入控制，并为每个 QoS-VPN 维护成员关系信息表，连接关系信息表和相关的信令以便实现成员关系自动发现和单边配置。

下面介绍 VPN－LBN 的划分方式。

为保证 QoS-VPN 网络可靠传送，有必要将 QoS-VPN 业务和尽力转发（Best effort）业务（包括没有 QoS 需求的 VPN 业务以及普通

Internet 业务）在资源分配和路由方面分开，QoS-VPN 的资源在预配置的 VPN-LBN 中分配并通过 VPN-CRC 选择显式路由，而 Best effort 的 VPN 业务仍然在剩下的没有分配的网络资源中遵循传统的 VPN 机制进行路由和转发。

如图 5 表示，VPN-LBN 由 PE、ITR、CR 以及连接这些路由器的 LSP 组成，LSP 可以静态配置或者根据容量规划和流量测量数据动态建立。

为进行 LSP 的保护或者容量的改变，MPLS TE 如快速重路由（Fast Reroute，简称“FRR”）等技术可以用于动态调整 LSP 带宽，并维护 VPN-LBN 拓扑。

当 QoS-VPN 的本地站点到远端站点的业务请求从 PE 传送到 VPN-CRC，根据用户和运营商之间的服务水平协议（Service Level Agreement，简称“SLA”）确定的相应的 QoS 需求也随着该业务请求传送到 VPN-CRC，VPN-CRC（如有必要，需要 VPN 承载控制网中其他 VPN-CRC 的参与）根据网络资源情况确定是否允许接入，如果允许接入，VPN-CRC 将计算能够满足 QoS 要求的路由，并将路由信息发送给入口 PE，路由信息是一个代表一组从入口 PE 到出口 PE 的串联的 LSP，入口 PE 将记录这些路由信息和所属的 QoS-VPN（通过 VPN-ID）和本地站点与远端站点（通过站点 ID），所有属于该 QoS-VPN 和本地站点到远端站点的业务都通过该路由进行转发，除非入口 PE 收到另外的路由指示。

入口 PE 从接口或子接口等相关信息识别 QoS-VPN，当一个 QoS-VPN 业务流进入网络后，入口 PE 获得流描述信息（通常包括源地址，源端口，目的地址，目的端口，协议类型），然后将包/帧用 VPN-CRC 指示的标签栈进行封装，对不同的数据类型（语音/视频/数据）为标签栈中所有的标签设置不同的 EXP 位组，并将数据包/帧引入 VPN-LBN，当数据流在路由上的 ITR 中传送时，均遵循

DiffServ-aware MPLS 技术。

下面详细介绍本发明方案中最重要的设备——VPN－CRC。

VPN 承载控制网由各域中的 VPN-CRC 组成，是 VPN 承载层的控制平面和管理平面，在本发明的一个较佳实施例中，VPN-CRC 应该具有如下功能：域内资源计算，路由选择，允许控制，域间资源请求，网络拓扑维护，成员关系信息维护，访问关系信息维护和自动发现，单边配置的信令等。而且，VPN-CRC 可以支持策略管理，SLA 管理，LSP 流量测量，以及和认证、授权和记帐服务器（Authentication Authorization and Accounting Server，简称“AAA Server”）的接口。

VPN－CRC 的内部结构及对外连接关系如图 6 所示。VPN－CRC 10 主要包含以下模块：

接口管理模块 111，用于实现并管理和外部设备进行通信的接口。例如与上游的 VPN－CRC 20、下游的 VPN－CRC 30、ITR 40 以及 ER 50 的通信。这些通信涉及到的协议将在下文中说明。

系统功能模块 112，用于提供支承整个 VPN－CRC 10 正常运行的底层平台。在本发明的一个较佳实施例中，该系统功能模块 112 是 VPN－CRC 10 中的操作系统。

协议处理模块 113，用于对 VPN－CRC 10 与各种外部设备通信的协议进行处理。并根据协议要求将通信数据转发给成员关系维护模块 114、拓扑和资源管理模块 115、路由管理模块 116 和自动发现信令模块 117，协议处理模块 113 通过接口管理模块 111 收发通信数据。

成员关系维护模块 114，用于维护成员关系信息表和访问关系信息表。成员关系信息表（membership information table）是包含属于同一 QoS-VPN 的站点成员的信息，该表是同一 QoS-VPN 中的站点 ID

的列表，通过 VPN-ID 索引。访问关系信息表（connectivity information table）包含同一 QoS-VPN 的成员之间的访问关系，即一个站点能够访问哪一些其他站点，该表可以通过成员信息表和每个站点的 Route Targets（路由目标）得到，如果同一个 QoS-VPN 中的一个站点的 export Route Target（输出路由目标）和另一个站点的 import Route Target（输入路由目标）相同，则这两个站点之间存在访问关系。在 VPN-CRC 10 进行允许控制时，需要参考访问关系信息表。通过访问关系信息表，QoS-VPN 站点之间可以组建全网状、Hub-Spoke 或者其它拓扑关系。

拓扑和资源管理模块 115，用于管理 VPN－LBN 的拓扑关系和资源。拓扑关系是 VPN－LBN 中各个节点的连接关系，资源主要是指这些连接关系上预留的带宽。VPN-LBN 的拓扑和资源的记录和维护独立于基础网络，VPN-LBN 的初始资源数据需要根据容量规划的结果手工配置。

路由管理模块 116，用于统一管理所有 QoS-VPN 的路由关系。

自动发现信令模块 117，用于变更的自动发现。自动发现是指访问关系信息并非人为配置在 VPN－CRC 10 中，而是由外部设备（如 PE）自动提供的。当自动发现信令模块 117 得到的信息中包括了成员关系或者 LBN 拓扑关系的变化，则自动发现信令模块 117 将通知成员关系维护模块 114 或拓扑和资源管理模块 115 进行相应的修改。

为维护和传送 QoS-VPN 的访问关系信息，VPN-CRC 需要维护 QoS-VPN 成员之间的访问关系，即 QoS-VPN 站点的拓扑，这可以通过（当然不限于）记录每个 QoS-VPN 的两个 site 列表来实现，一个是允许发送的站点列表，一个是允许接收的站点列表。为支持 QoS-VPN 成员关系和访问关系信息的修改的自动发现，在增加或删除 QoS-VPN 中的站点时，相关的更新消息应该在 PE 和 VPN-CRC 之间传送，涉及

到的 VPN-CRC 应该更新成员信息表和访问关系信息表。通过这种机制，可以实现单边配置，即在 QoS-VPN 站点增加或删除时或者站点之间的访问关系发生变化时，只需要对站点增删或者访问关系变化的一个站点的 PE 上进行配置，这些配置将触发更新消息在相关的 VPN-CRC 和 PE 上自动传送，接收到更新消息的 VPN-CRC 将更新对应的 QoS-VPN 成员关系信息表和访问关系信息表。

在增加 QoS-VPN 站点时，业务请求（包括 VPN-ID，本地站点 ID，远端站点 ID，QoS 要求）将传递到本域 VPN-CRC，VPN-CRC（如果必须，需要相关 VPN-CRC 参与）将为增加的站点访问其它站点计算资源，如果允许这些站点的增加，将计算这些新增站点访问其它站点的路由，并将路由指示给相关 PE，这些 PE 更新它们的 QoS-路由信息表，当远端 PE 感知到这些站点的增加，将触发它们自己的本地站点访问这些新增站点的业务请求，VPN 承载控制网将执行相同处理，最后所有站点将得知相互访问的路由信息。

在删除站点时，VPN-CRC 除了更新相关的成员关系信息表和访问关系信息表外，将释放和删除的站点相关的资源，并通知相关 PE 删除 QoS 路由信息表中相关条目，当远端 PE 感知到站点的删除，将触发它们关于自己的本地站点访问这些已删除站点的资源删除。

拓扑和资源表 118，用于存储 VPN－LBN 的拓扑关系和资源。

路由表 119，用于存储 QoS-VPN 的路由（实质上是各个站点可被访问的目的地址集合）。该目的地址集合由若干个地址前缀或地址组成。

VPN-CRC 从本域入口 PE 的业务请求（包括 VPN-ID，本端站点 ID，远端站点 ID，QoS 要求）或者其它 VPN-CRC 的资源请求时，将进行资源计算，路由选择和允许控制（如果需要，还要将资源请求传送到

下游 VPN-CRC），如果其中涉及到的某个 VPN-CRC 资源计算的结果是“拒绝 ”，需要将该响应一直向上游 VPN-CRC 传送，直到到达入口 PE。否则，需要将本 VPN-CRC 确定的路由信息向上游传送，直到将全程的路由信息（标签栈）发送给入口 PE。入口在转发从本端站点到远端站点的数据时，根据 CE 到 PE 的业务流的描述设置标签栈中所有标签的 EXP 位组，这样，从本端站点到远端站点的业务都从上述计算的路由上传送，但相同方向不同类型的业务通过 EXP 位组区分，按照 MPLS-DiffServ 机制传送。

下面说明对图 4 中 VPN 承载层中的 PE、ITR 和 CR 的功能需求。

PE 应该支持静态 LSP 配置或者通过 CR-LDP/RSVP-TE 动态建立 LSP 以便实现预配置以及 VPN-LBN 的动态调整，而且应该支持流分类，以便能为从 VPN-CRC 接收到的标签栈设置 EXP 位组。PE 中保存了 QoS 路由信息表，该表主要保存了以下信息：VPN－ID，本地站点，远端站点（远端站点中可以访问的目的地址集合），本地站点和远端站点之间的路由。

当从 VPN-CRC 接收到允许控制响应，如果响应是“允许接入”，路由和 QoS 信息将包含在内，入口 PE 在 QoS 信息表中将记录这些信息，它为每个 QoS-VPN 分别维护这些信息，根据 VPN-ID 索引，在每个 QoS-VPN 的信息中，为每个站点对（一个本地站点到一个远端站点）记录一个条目，根据 QoS 路由信息表，入口 PE 进行队列，调度，整形，标记，策略，MPLS 封装，然后在 VPN-LBN 中根据标签栈确定的路由进行转发。

中间传送路由器 ITR 应该支持静态 LSP 配置或者通过 CR-LDP/RSVP-TE 动态建立 LSP 以便实现预配置以及 VPN-LBN 的动态调整，而且应该支持 DiffServ-aware MPLS 和按类型处理流。

IP 骨干网络中的核心路由器 CR 只需要支持 DiffServ-aware MPLS 和按类型处理流。

下面说明借助 VPN 地址进行 QoS - VPN 之间隔离的方法。

VPN 地址可以由 VPN-LBN 中全局唯一的 VPN-ID 和 L3/L2/L1 VPN 相关的私有地址组成，如，L3 VPN 中的 IPV4/IPV6/IPX 地址，L2 VPN 中的数据链路地址，L1VPN 中的交叉连接标识，在这种 VPN 地址方案中，不同 QoS-VPN 中各站点的地址可以重叠，由于 VPN-ID 在 VPN-LBN 中全局唯一，组成的 VPN 地址也将在 VPN-LBN 内唯一。

QoS 路由信息表可以通过 VPN-ID 区分不同 QoS-VPN 的信息，从而实现 QoS-VPN 之间的隔离。

下面说明路由和转发的方法。

QoS-VPN 路由在 PE 的 QoS 路由信息表中维护，其粒度是 QoS-VPN 的站点对，即一个本地站点到一个远端站点之间的所有业务的路由相同，在入口 PE 的路由查找是分为两级的，第一级根据不同 VPN-ID 索引，找到与本地站点所属的 QoS-VPN，第二级查找搜索针对该 QoS-VPN 中的本地站点和远端站点对，和远端站点关联的是远端站点中的聚合地址，当业务流中的目的地址和站点对中与远端站点关联的聚合地址匹配时，认为搜索成功。在两级查找成功后，入口 PE 为该业务流确定路由信息（VPN-CRC 指定的 MPLS 标签栈），并标记路由信息标签中的 EXP 位组。如果，两级查找之一失败，则入口 PE 可以拒绝该业务流。

QoS-VPN 转发基于 MPLS 技术，使用 VPN-CRC 下发的标签栈和入口 PE 为业务流设置的 EXP 位组，根据外层标签采用 MPLS-DiffServ 机制，保证了业务带宽和转发优先级，从而保证了 QoS-VPN 的服务质量（带宽，时延，抖动，丢包率）。

下面说明各个设备之间的接口和信令需求，包括 PE 和 CE 之间、VPN-CRC 和运营商路由器(包括 PE, ITR, CR)之间, VPN-CRC 和 VPN-CRC 之间的接口和协议。

PE 和 CE 之间的接口传送用户信息，如拓扑，CE 连接的站点的聚合的私有地址（如 L3VPN 中的私有 IPv4/IPv6/IPX 地址，L2VPN 中的数据链路地址，L1VPN 中的交叉连接标识），业务请求（包括流标识）。

VPN-CRC 和 PE 之间的接口允许 VPN-CRC 指示 PE 处理每个站点的业务流，有必要为该借口规定相应的协议，可以在 COPS 基础上根据本文中的结构扩展。

该协议需要支持如下功能:

(1) 入口 PE 向 VPN-CRC 发送业务请求（包括 VPN-ID，本地站点 ID，export Route Target，远端站点 ID，QoS 要求），QoS 要求包括业务类型及其带宽，优先级，时延，抖动限制，丢失率限制，MTU 等，它根据用户和运营商之间的 SLA 确定针对每个站点的服务质量要求。

(2) VPN-CRC 根据业务请求中的站点 ID 和 export Route Target 确定本地站点和远端站点之间是否存在访问关系（VPN-CRC 需要将业务请求信息传递到相关的 VPN-CRC 和出口 PE），在存在访问关系时，无论 VPN 承载控制网的允许控制结果是“拒绝”或“接受”，都将该结果通知入口 PE。

(3) 在允许控制“允许”时，VPN-CRC 将关于该站点对的路由(表示一组串联 LSP 的标签栈)通知给入口 PE, PE 在 QoS 路由信息表中为每个 QoS-VPN 的每个站点对创建该记录。

(4) 在为 QoS-VPN 中增加或删除站点时，或者站点间的访问关系变化时，变化发生站点对应的 PE 应向本域 VPN-CRC 发送更新消息，VPN-CRC 向相邻 VPN-CRC 传递该消息，最终发送给对端 PE，相关的

VPN-CRC 将更新成员关系信息表和访问关系信息表，相关的 PE 将更新 QoS 路由信息表中的相应表项。

(5) PE 将它所连接站点的聚合 VPN 地址信息发送给 VPN-CRC，VPN-CRC 在 VPN 承载控制网中发布，并最终发布给相关的 PE，该功能可以通过扩展现有的 BGP 协议实现，最后，所有 PE 将在 QoS 路由信息表中保存它所接入的 QoS-VPN 各站点的聚合 VPN 地址，当 PE 收到业务流时，可以根据 QoS 路由信息表和流标识确定路由和 EXP 位组。

而且，VPN-CRC 和域内 PE，ITR，CR 之间的接口应该支持如下功能:

(1) 允许 VPN-CRC 为每种业务类别配置 MPLS DiffServ PHB。

(2) 允许 PE/ITR/CR 等路由器向 VPN-CRC 报告 LSP 状态，当链路或路由器发生故障时，路由器将向本域 VPN-CRC 上报，VPN-CRC 将这些故障信息在 VPN 承载控制网中发布，这些 VPN-CRC 重新为它们预留的路由计算资源，当一些路由需要更新时，VPN-CRC 应该将新路由发送给相关入口 PE。

VPN-CRC 之间的接口用于实现跨域的 QoS-VPN 站点之间业务的资源分配和路由选择。

有必要为该接口定义单独的协议，可以对 COPS 或者 BGP 进行扩展来完成相应的功能。

该协议需要支持如下功能:

(1) 允许 VPN-CRC 向下游 VPN-CRC 申请为跨域 QoS-VPN 站点之间的业务分配承载资源。

(2) 允许 VPN-CRC 将域间的 QoS-VPN 业务标识信息(本地站点 ID，远端站点 ID，VPN-ID) 通知给下游 VPN-CRC。

(3)允许 VPN-CRC 将 域间的 QoS-VPN 业务的 QoS 需求(包括业务类型及其带宽，优先级，时延限制，抖动限制，丢失率限制等)通知给下游 VPN-CRC。

(4)允许 VPN-CRC 请求相邻的 VPN 释放为域间的 QoS-VPN 业务分配的承载资源。

(5)允许 VPN-CRC 向其它 VPN-CRC 查询它为域间 QoS-VPN 业务的资源分配状态。

(6)允许 VPN-CRC 向其他 VPN-CRC 通知查询响应。

(7)允许 VPN-CRC 和其他 VPN-CRC 交换域间业务等级规格(service level specification，简称“SLS”)和路由信息。

下面讨论混合 QoS-VPN 的情况。

在某些情况下，VPN 的一些站点有 QoS 要求，而其他站点没有 QoS 要求，这种 VPN 称为混合 QoS-VPN。混合 QoS-VPN 可以分为两部分，一部分由那些有 QoS 要求的站点组成，称为 sub-QoS-VPN，另一部分由那些没有 QoS 要求的站点组成，称为 sub-VPN。对于 sub-QoS-VPN，其 QoS 保证可以采用上述集中资源控制保证 QoS 的 MPLS NBVPN 方案，对于 sub-VPN，仍然遵循 IETF L3VPN/L2VPN 工作组的相关 RFC 和 draft 来实现。Route Target 用于确定整个 VPN(包括 sub-QoS-VPN 和 sub-VPN)的访问关系，可以采用 VPN-CRC 来确定，另外引入 QoS Route Target(有 QoS 需求的路由目标)来维护 sub-QoS-VPN 的访问关系信息表，QoS Route Targets 和 Route Targets 格式相同，比较了 Route Target 确定站点之间的普通访问关系后，继续比较 QoS Route Target(如果两个站点之一的业务请求中存在)，如果比较通过，则这两个站点之间的业务具有 QoS 要求，这两个站点都属于 sub-QoS-VPN。否则将它们归为 sub-VPN。

下面讨论域内 QoS-VPN 和域间 QoS-VPN 的情况。

域内 QoS-VPN 路由选择和域间路由是资源管理和允许控制的基础。

VPN-CRC 通过在拓扑信息表和资源信息表中进行域内路由选择，路由选择的算法可以是固定的，例如时间相关路由（Time Dependent Routing，简称“TDR”）/状态相关路由（State Dependent Routing，简称“SDR”）。而且，VPN-CRC 中应该维护一个域间路由表用于通过 QoS 信令协议确定域间 LSP，以发现相邻的下游 VPN-CRC。

VPN-CRC 的域间路由表可以手工配置或运行动态路由协议自动产生。

下面讨论跨不同网络提供商如何提供 QoS-VPN。

为了在不同提供商的网络中支持 QoS-VPN，他们的自治系统边界路由器（Autonomous System Boundary Router，简称“ASBR”）应该互通以传送 VPN 业务请求信令和 VPN 业务。如果双方网络都部署了 VPN-CRC，他们的 VPN-CRC 可以互通，此时，这些 VPN-CRC 之间仅交换和映射网间 SLA，此时，VPN-CRC 仅管理网内链路资源，ASBR 通过规定的 SLA 管理网间链路资源，完成运营商内部 QoS-VPN 情况下的入口 PE 的功能，如果其中一个网络运营商没有部署 VPN-CRC，而是采用了其他的 QoS 机制，两个 ASBR 应该相互映射 QoS 需求，则最终 QoS 保证的程度将依赖于其他网络提供商的 VPN QoS 实现机制。

虽然通过参照本发明的某些优选实施例，已经对本发明进行了图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种各样的改变，而不偏离所附权利要求书所限定的本发明的精神和范围。

权 利 要 求

1. 一种虚拟专用网中保证服务质量的系统，其特征在于，包含:

逻辑承载网，使用多协议标签交换技术通过在基础 IP 网络中配置预留带宽的标签交换路径连接各种路由器而形成，专用于传输有服务质量需求的业务;

承载控制网，用于对所述逻辑承载网进行维护，为所述业务分配所述路由，以及将该业务的优先级标记到封装到该业务数据流的多协议标签交换数据包的路由标签的服务质量字段中，并按照所述分配的路由，使所述业务通过所述逻辑承载网路由到需发送的对端。

2. 根据权利要求 1 所述的虚拟专用网中保证服务质量的系统，其特征在于，所述承载控制网包含集中式资源控制器，用于管理所述逻辑承载网的网络资源，维护所述逻辑承载网的网络拓扑，进行资源计算和业务路由选择，为所述路由器发送业务路由指示，在所述逻辑承载网内分配资源并进行接入控制，为每一个所述虚拟专用网维护成员关系信息和连接关系信息，实现成员关系的自动发现和单边配置。

3. 根据权利要求 2 所述的虚拟专用网中保证服务质量的系统，其特征在于，所述集中式资源控制器在所述逻辑承载网的每一个域中部署一个，各个所述集中式资源控制器相互连接，交流所述逻辑承载网的拓扑、资源信息以及所述虚拟专用网的路由信息。

4. 根据权利要求 1 所述的虚拟专用网中保证服务质量的系统，其特征在于，所述逻辑承载网和所述承载控制网通过带外的方式发布所述虚拟专用网的路由、维护所述虚拟专用网的成员关系、维护所述虚拟专用网各站点之间的访问关系。

5. 根据权利要求 2 所述的虚拟专用网中保证服务质量的系统，其特征在于，所述各种路由器包括骨干网边缘路由器、中间转接路由器与核心路由器，其中:

所述骨干网边缘路由器：用于识别有服务质量需求的虚拟专用网，并对从该虚拟专用网进入的有服务质量需求的业务用所述集中式资源控制器指示的标签栈进行封装，然后根据该业务的优先级设置所述标签栈中所有标签的服务质量字段，将封装好的业务数据包通过所述逻辑承载网传输；

所述中间转接路由器：用于标签交换路径的静态或动态配置、以及区别服务模式的多协议标签交换和按类型处理流；

所述核心路由器：用于区别服务模式的多协议标签交换和按类型处理流。

6. 根据权利要求 2 所述的虚拟专用网中保证服务质量的系统，其特征在于，所述集中式资源控制器包含接口管理模块、协议处理模块、成员关系维护模块、拓扑和资源管理模块、路由管理模块和自动发现信令模块，其中：

所述接口管理模块用于实现并管理虚拟专用网和外部设备进行通信的接口；

所述协议处理模块用于对所述集中式资源控制器与各种外部设备通信的协议进行处理，并根据协议要求将通信数据转发给所述成员关系维护模块、拓扑和资源管理模块、路由管理模块和自动发现信令模块，所述协议处理模块通过所述接口管理模块收发通信数据；

所述成员关系维护模块用于维护所述虚拟专用网的成员关系信息和所述虚拟专用网站点间访问关系信息；

所述拓扑和资源管理模块用于管理所述逻辑承载网的拓扑关系和资源；

所述路由管理模块用于管理所述虚拟专用网的路由关系；

所述自动发现信令模块用于变更的自动发现，并通知所述成员关系维护模块、所述拓扑和资源管理模块修正相应的信息。

7. 一种虚拟专用网中保证服务质量的方法，其特征在于，包含以下步骤：

A 在基础 IP 网络中，使用多协议标签交换技术通过配置预留带宽的标签交换路径构造逻辑承载网，该逻辑承载网专用于传输有服务质量需求的业务；

B 部署用于集中管理所述逻辑承载网资源的集中式资源控制器；

C 需要传输有服务质量需求的业务时，将该业务的优先级标记到封装该业务数据流的多协议标签交换数据包的路由标签栈的服务质量字段中，按照所述集中式资源控制器分配的路由，通过所述逻辑承载网路由到需发送的对端。

8. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，其特征在于，步骤 B 和步骤 C 之间还包括：集中式资源控制器计算并下发站点之间的访问路至虚拟专用网的路由器，以便所述路由器保存集中式资源控制器分配的路由。

9. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，其特征在于，所述路由是由标签栈确定的串行标签交换路径。

10. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，其特征在于，所述步骤 C 中，对所述业务路由标签栈中全部标签的服务质量字段设置相同的数值。

11. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，其特征在于，所述方法还包括：使用多协议标签交换流量工程技术动态调整所述逻辑承载网的拓扑和资源。

12. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，其特征在于，在所述步骤 C 中，所述业务的优先级是由所述业务的类型确定的。

13. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，

其特征在于还包括以下步骤:

判断业务的收、发站点是否都有服务质量需求，如果是则使用逻辑承载网内的资源传输该业务，否则使用所述基础 IP 网络的其他资源传输该业务。

14. 根据权利要求 13 所述的虚拟专用网中保证服务质量的方法，其特征在于，在对业务的收、发站点进行是否都有服务质量需求的判断前还包括以下子步骤:

比较所述收、发站点的路由目标，判断所述收、发站点是否为普通访问关系，如果是则进入后续步骤，否则结束。

15、如权利要求 13 所述的虚拟专用网中保证服务质量的方法，其特征在于，判断业务的收、发站点是否都有服务质量需求是通过以下方式来判断的: 通过比较所述收、发站点的路由目标，判断所述收、发站点是否为有服务质量需求的访问关系，若是，则业务的收、发站点都有服务质量需求，否则，业务的收、发站点未有服务质量需求。。

16. 根据权利要求 7 所述的虚拟专用网中保证服务质量的方法，其特征在于，所述集中式资源控制器为每一对有服务质量需求的站点分配的路由唯一。

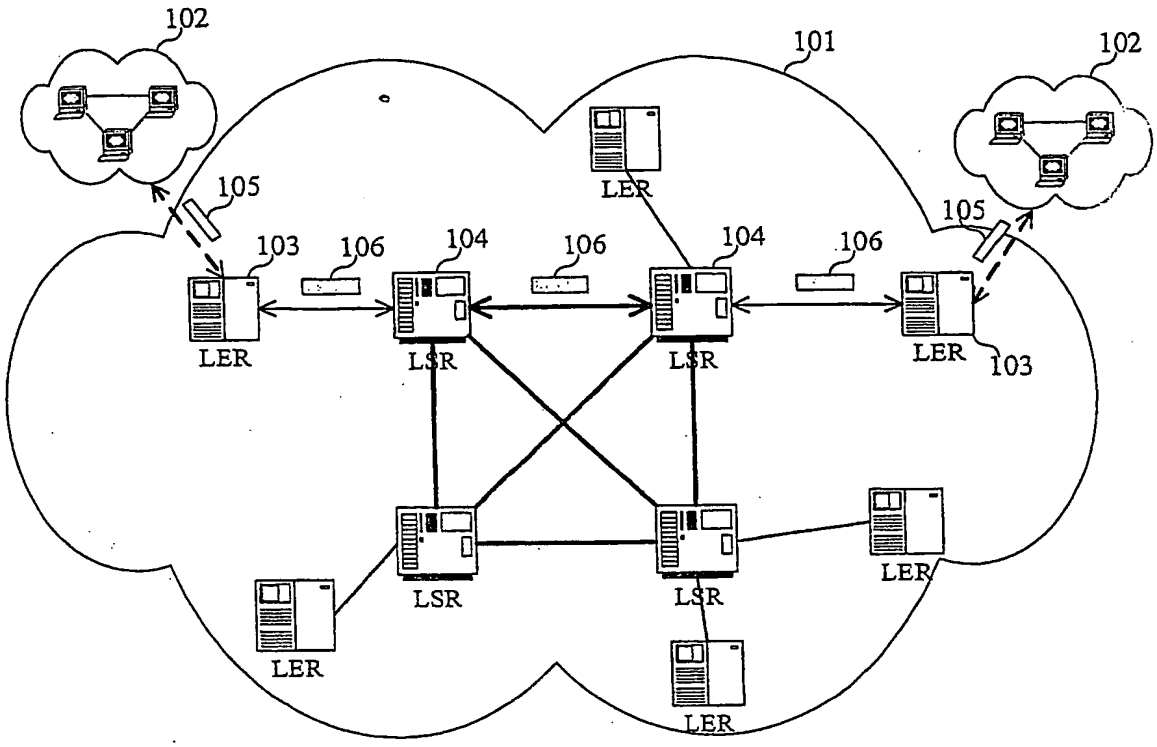
102
101
102
105
LER
105
103
106
104
106
104
106
LER
LSR
LSR
LER
103
LSR
LSR
LER
LER
LER

图 1

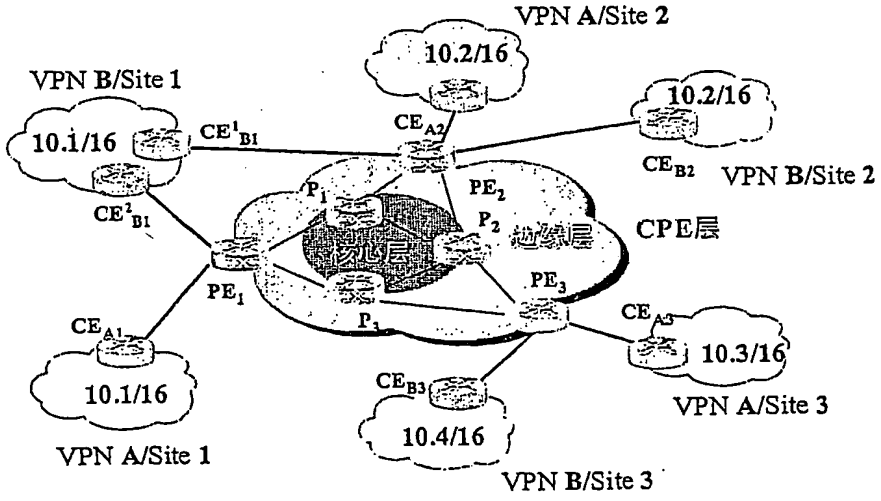
VPN A/Site 2
10.2/16
VPN B/Site 1
10.1/16
CE¹B1
CEA2
10.2/16
CEB2
VPN B/Site 2
CE¹B1
P1
PE2
P2
核心层
边缘层
CPE层
PE1
PE3
P3
CEA1
CEA3
10.3/16
10.1/16
CEB3
10.4/16
VPN A/Site 3
VPN A/Site 1
VPN B/Site 3

图 2

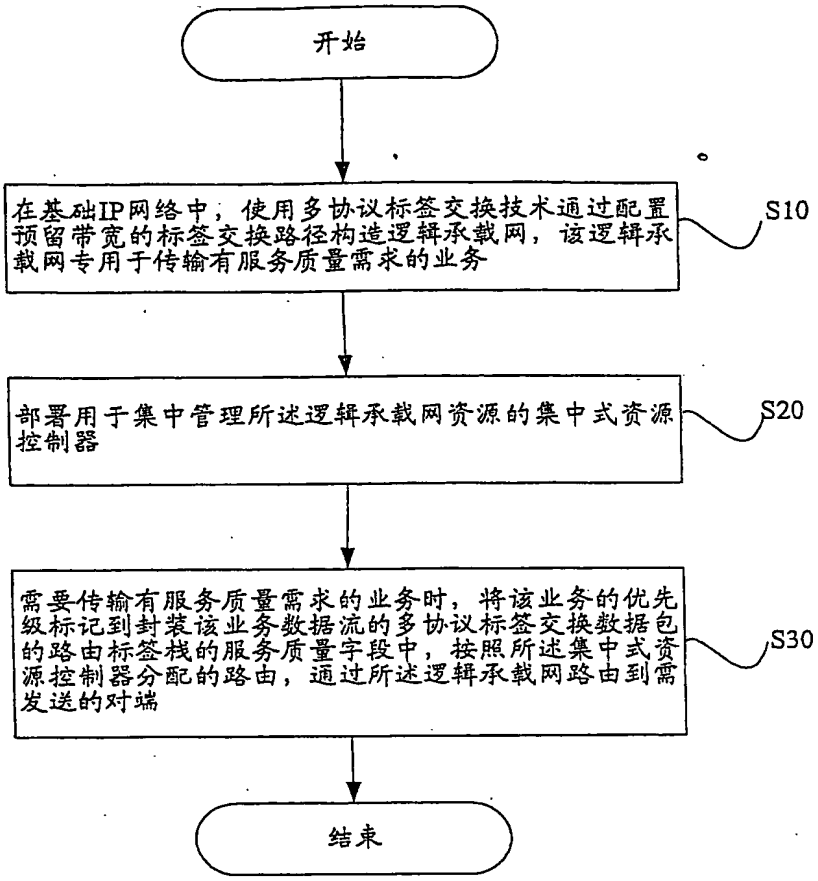
开始
在基础IP网络中，使用多协议标签交换技术通过配置预留带宽的标签交换路径构造逻辑承载网，该逻辑承载网专用于传输有服务质量需求的业务
S10
部署用于集中管理所述逻辑承载网资源的集中式资源控制器
S20
需要传输有服务质量需求的业务时，将该业务的优先级标记到封装该业务数据流的多协议标签交换数据包的路由标签栈的服务质量字段中，按照所述集中式资源控制器分配的路由，通过所述逻辑承载网路由到需发送的对端
S30
结束

图 3A

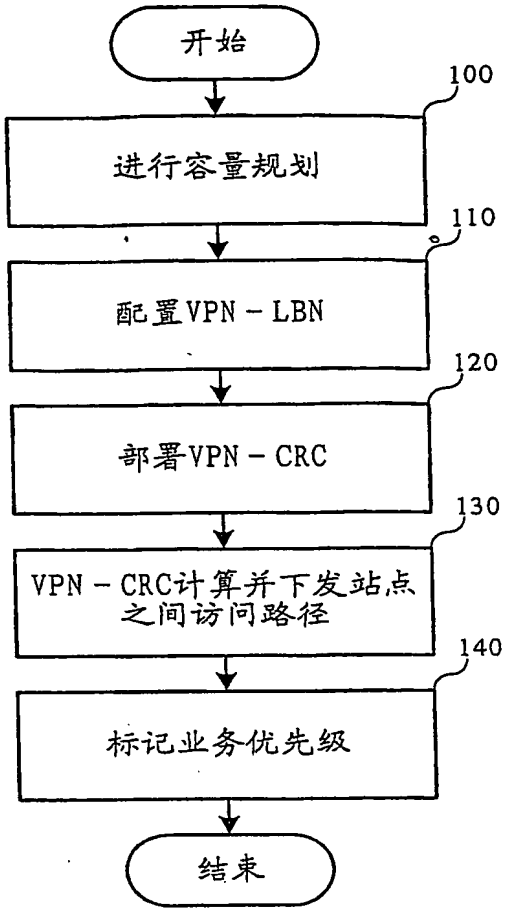
开始
100
进行容量规划
110
配置VPN－LBN
120
部署VPN－CRC
130
VPN－CRC计算并下发站点之间访问路径
140
标记业务优先级
结束

图 3B

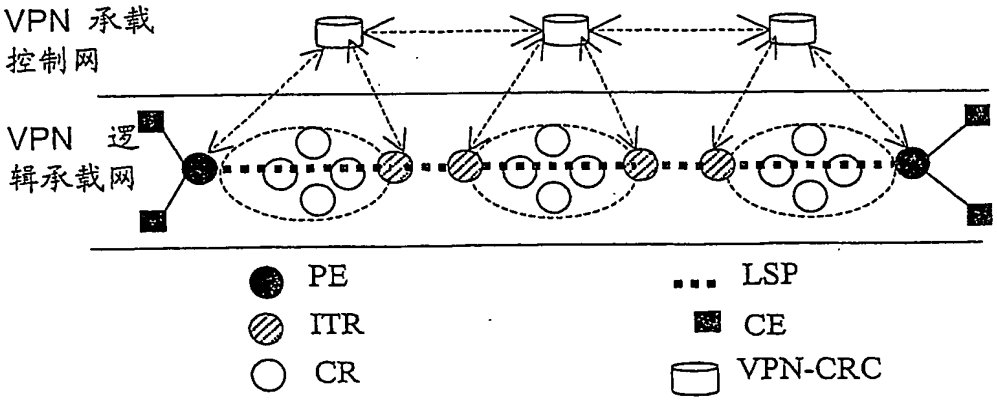
VPN 承载控制网
VPN 逻辑承载网
PE
ITR
CR
LSP
CE
VPN-CRC

图 4

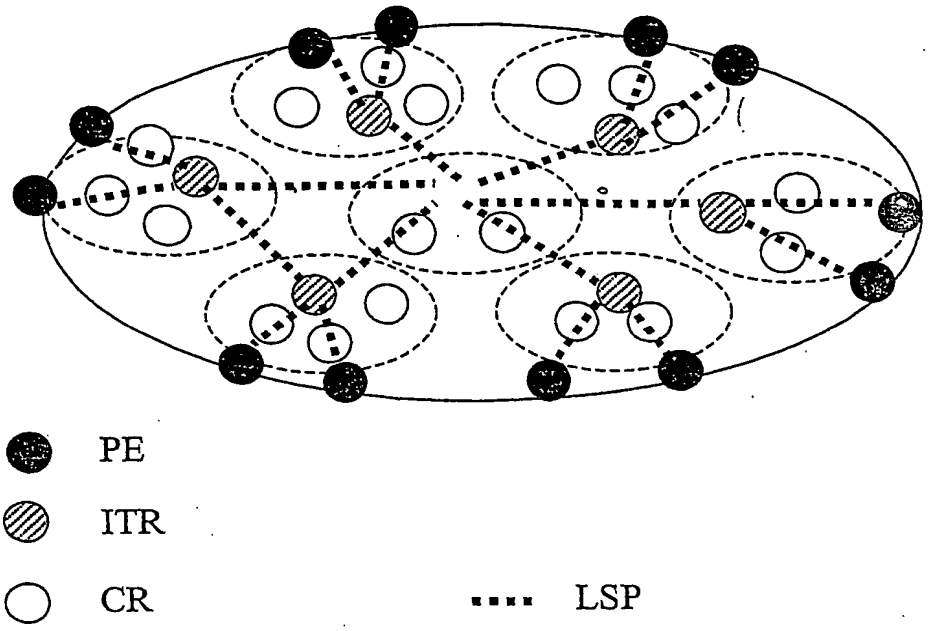
PE
ITR
CR
LSP

图5

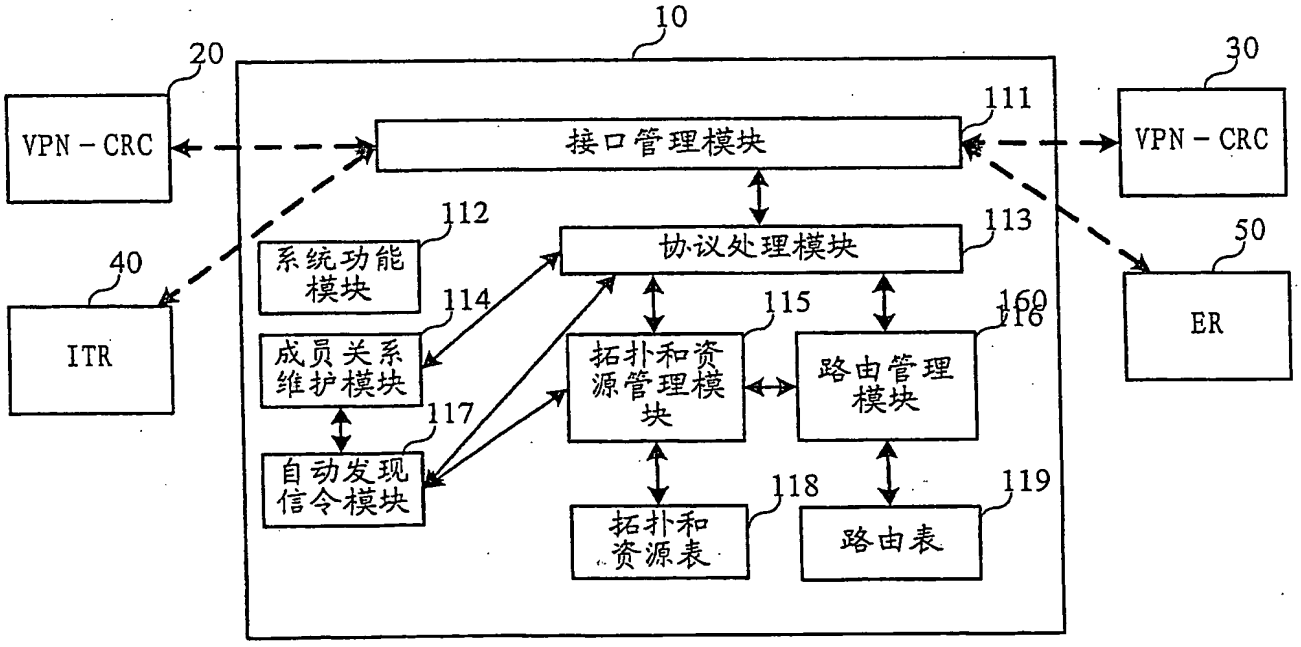
10
20
VPN－CRC
30
VPN－CRC
111
接口管理模块
112
系统功能模块
113
协议处理模块
40
ITR
50
ER
114
成员关系维护模块
115
拓扑和资源管理模块
160
116
路由管理模块
117
自动发现信令模块
118
拓扑和资源表
119
路由表

图6